CONTROLLED MAINTENANCE

Controlled maintenance requires that the appropriate procedures for system maintenance are followed and implemented by the designated University OIT personnel.

TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Contacts</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stakeholder(s)</td>
<td>1</td>
</tr>
<tr>
<td>Purpose</td>
<td>2</td>
</tr>
<tr>
<td>Requirements</td>
<td>2</td>
</tr>
<tr>
<td>Violations</td>
<td>2</td>
</tr>
<tr>
<td>Interpretation</td>
<td>2</td>
</tr>
<tr>
<td>Publication</td>
<td>2</td>
</tr>
<tr>
<td>Review Schedule</td>
<td>3</td>
</tr>
<tr>
<td>Related Documents</td>
<td>3</td>
</tr>
</tbody>
</table>

CONTACT(S)

Office of Information Technology – (757)823-2869

STAKEHOLDER(S)

University Faculty & Staff
Office of Information Technology
PURPOSE
This control is intended to establish the policy and procedures for the security aspects of the University’s information system maintenance program.

REQUIREMENTS

NSU:

1. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or University requirements;

2. Controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;

3. Requires that a designated official explicitly approve the removal of the information system or system components from University facilities for off-site maintenance or repairs;

4. Sanitizes equipment to remove all information from associated media prior to removal from University facilities for off-site maintenance or repairs; and

5. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

VIOLATIONS

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 32-01 and Department of Human Resources Management Policy 1.75. The appropriate level of disciplinary action will be determined on an individual case basis by the appropriate executive or designee, with sanctions up to or including termination or expulsion depending upon the severity of the offense.

INTERPRETATION

The Information Security Officer is responsible for official interpretation of this policy. Questions regarding the application of this policy should be directed to the Office of Information Technology. The Information Security Officer reserves the right to revise or eliminate this policy.

PUBLICATION

This policy shall be widely published and distributed to the University community. To ensure timely publication and distribution thereof, the Responsible Office will make every effort to:

1. Communicate the policy in writing, electronic or otherwise, to the University community within 14 days of approval;
2. Submit the policy for inclusion in the online Policy Library within 14 days of approval;

3. Post the policy on the appropriate SharePoint Site and/or Website; and

4. Educate and train all stakeholders and appropriate audiences on the policy’s content, as necessary. Failure to meet the publication requirements does not invalidate this policy.

REVIEW SCHEDULE

- Next Scheduled Review: 05/28/2015
- Approval by, date: Office of Information Technology and 05/28/2014
- Revision History:

- Supersedes (previous policy): OIT 62.8.902 Controlled Maintenance

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard